Please replace the paragraph bridging pages 1 and 2 (page 1, line 15 through page 2, line 4) with the following rewritten paragraph:

a2

The traditional DES is a block cipher, which acts on independent fixed-length, plaintext input blocks and yields fixed-length output blocks. That is, the DES encryption process maps 64-bit plaintext input blocks into 64-bit ciphertext output blocks. There are 2^{56} (i.e. $10^{16.8}$) mappings where each mapping selected by a 56-bit keying variable is unique and invertible. The DES decryption is a reverse of the encryption mapping, and requires knowledge of the specific keying variable used in the encryption process.

Please replace the paragraph beginning at page 2, line 5 with the following rewritten paragraph:

a3

The use of the DES as a cryptographic system is built around its most basic mode, which is known as the Electronic Code Book (ECB) mode. Other modes of DES, such as Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB), are described in the Federal Information Processing Standards Publication (FIPS PUB) number 81. In the ECB mode, a 64-bit plaintext word is converted to a 64-bit ciphertext word. This conversion is a one-to one and reverse mapping is electable. This conversion is also done under the control of a 56-bit keying variable. The keying variable for the DES is generally given as 64-bits with the convention of using 8 bits as the odd parity bits.

Please replace the paragraph beginning at page 3, line 1 with the following rewritten paragraph:

a4 With the inexorable advance in available worldwide computer power coupled with the existing fame of the DES algorithm, it was inevitable that the DES algorithm would continue to draw attention and challenges as to its sufficiency in protecting data at the highest level. In particular, challenges have been mounted through parallel exhaustive attack and so-called special attacks in which one seeks to find a path to a solution that is computationally less than that of simple exhaustion.

Please replace the paragraph beginning at page 3, line 7 with the following rewritten paragraph:

a5 There are two important publications with respect to cryptanalysis of the DES cryptoprinciple. The publications represent two very powerful distinct cryptanalytic approaches. Neither approach was initially successful at defeating the DES but both approaches deserve consideration as genres of potent cryptanalysis. The first of these was reported in the paper "Exhaustive Cryptanalysis of the NBS Data Encryption Standard" by W. Diffie and M. Hellman (Computer June 12977, pp. 74-84). This paper discussed the construction of a large parallel processor in which the entire 56-bit keying variable space was partitioned over a very large number of identical independent processors. The paper also advanced the argument that declining computation costs would eventually reduce the cost of a solution to a nominal sum.

Please replace the paragraph beginning at page 3, line 17 with the following rewritten paragraph:

a6

This type of attack can be countered, of course, by increasing the size of the keying variable and it would not require a variable of much larger size than the 56-bit variable to effectively frustrate this approach.

Please replace the paragraph beginning at page 4, line 14 with the following rewritten paragraph:

a7

(2) the attacks on DES with 9-16 rounds are not influenced by the P permutation and the replacement of the P permutation by any other fixed permutation or function cannot make them less successful;

Please replace the paragraph beginning at page 5, line 4 with the following rewritten paragraph:

a8

Further work related to differential cryptanalysis encompasses so called linear cryptanalysis ("Linear Cryptanalysis Method for DES Cipher," Mistura Matsui, Abstracts of EUROCRYPT '93, pp. W112-123) and statistical attacks by Davis and others. Biham and Shamir published an improvement of one of these attacks in "An Improvement of Davies' Attack on DES," EUROCRYPT '94, pp. 461-467. In this paper they reported breaking the full 16-round DES faster than exhaustive search. The statistical attack requires a larger volume of known plaintext-ciphertext pairs.

Please replace the paragraph beginning at page 6, line 3 with the following rewritten paragraph:

a9

Also from FIPS PUB 46-3: "DES forms the basis for TDEA (Triple Data Encryption Algorithm or Triple DES)." "The X9.52 standard, "Triple Data Encryption Algorithm Modes of Operation" describes seven different modes for using TDEA (Triple Data Encryption Algorithm or Triple DES) described in this standard. These seven modes are called the TDEA Electronic Codebook Mode of Operation (TECB) mode, the TDEA Cipher Block Chaining Mode of Operation (TCBC), the TDEA Cipher Block Chaining Mode of Operation - Interleaved (TCBC-I), the TDEA Cipher Feedback Mode of Operation (TCFB), the TDEA Cipher Feedback Mode of Operation - Pipelined (TCFB-P), the TDEA Output Feedback Mode of Operation (TOFB), and the TDEA Output Feedback Mode of Operation - Interleaved (TOFB-I). The TECB, TCBC, TCFB and TOFB modes are based upon the ECB, CBC, CFB and OFB modes respectively obtained by substituting the DES encryption/decryption operation with the TDEA encryption/decryption operation.

Please replace the paragraph beginning at page 7, line 10 with the following rewritten paragraph:

a10

2. Triple DES will be the FIPS approved symmetric encryption algorithm of choice.

Please replace the paragraph bridging pages 8-10 (line 10, page 8 through line 2, page 10) with the following rewritten paragraph:

a11

The enhanced DES cryptographic system of the present invention uses modifications to improve on the conventional DES which allows for increased levels of security for each of the four single DES modes (i.e., ECB, CBC, CFB and OFB) while incorporating a form that may be made compatible with the traditional 56 bit DES/DEA algorithm. DEA (Data Encryption Algorithm) is the term used by ANSI and the international community to identify DES. Similarly the enhanced DES cryptographic system and process of the present invention can improve on the TDEA by allowing for increased levels of security for each of the seven modes using the enhanced DES system as a basis while incorporating forms that are compatible with the traditional seven TDEA modes called the TDEA Electronic Codebook Mode of Operation (TECB) mode, the TDEA Cipher Block Chaining Mode of Operation (TCBC), the TDEA Cipher Block Chaining Mode of Operation - Interleaved (TCBC-I), the TDEA Cipher Feedback Mode of Operation (TCFB), the TDEA Cipher Feedback Mode of Operation - Pipelined (TCFB-P), the TDEA Output Feedback Mode of Operation (TOFB), and the TDEA Output Feedback Mode of Operation - Interleaved (TOFB-I). The enhanced algorithm modifies the fixed permutation P of the classic DES algorithm that is applied after the S

A11

boxes while preserving its character of a 1-1 mapping. One of the preferred embodiments utilizes a logical array of binary switches in a structured class of networks (e.g. Omega networks or Benes-Waksman networks) so as to construct permutations which can vary. Depending upon the particular network implemented, a related fixed permutation may be computed so that when the binary switches are all set to a default condition, the resulting permutation created by the network when followed by the related fixed permutation, results in a permutation equivalent to the fixed permutation of the conventional DES. This is a means used to create the feature of "backward compatibility" with the traditional single DES or the traditional modes of TDEA. These variable permutations can be based upon elements of the cryptographic key (i.e. cryptovariable), or can depend on additional elements such as an encipherment counter or frame counter or some permanently fixed bits. Although there are many logically equivalent ways to implement the variable permutation which are all compatible as long as the logical structure is maintained, the enhancement of the present invention is such that as long as the permutation is kept secret and not known by unauthorized parties, the permutation could be varied less frequently than the life of the 56 bit cryptographic key for the single DES, or it can be changed at the beginning of a cryptoperiod and not changed until the next cryptoperiod or it could be varied within the cryptoperiod based upon such factors or various combinations of the following such factors as additional bits from a cryptographic key, a clock or counter, specified number of output bits from the encryption engine after every set of 16 rounds of the engine, or within engine's operating cycle at each separate "round" of the engine. Of course, these additional elements must also be known by the "decrypt" engine.

Please replace the paragraph beginning at page 10, line 3 with the following rewritten paragraph:

a12

It is well known to persons skilled in the art that various cryptographic devices can be used to generate bit streams and vectors for other cryptographic purposes than message encryption and decryption such as symmetric keys for other cryptographic devices or initialization vectors. Some schemes use randomizers or noise diodes which produce non deterministic outputs that can be used for cryptographic keys and or starting settings or initialization vectors for cryptographic devices. In these types of applications it is not necessary nor is it desirable to communicate the initial settings, cipher keys and randomizer bits of the cipher machine used as this type of bit stream generator to any other cipher machine. In the applicants' enhanced device a preferred method of utilizing such randomizer output bits is in the generation of the P* permutation where the randomizer bits are used directly or indirectly (e.g. setting a maximal length LFSR) for beta elements in an Omega network and to also be used in determining when to replace the P* permutation with another P*. One of the traditional concerns has been that a biased (i.e. not exactly 50% ones and 50% zeros) randomizer when used for the initialization of a cipher device may cause biased or partially predictable outputs. The same concern occurs when the randomizer is used to directly produce cryptographic keys used by a cryptographic device to generate so called random output. Using the non-deterministic output of a randomizer to generate and or replace the P* permutation provides additional assurance against any such biased or partially predictable output from the enhanced device of the present invention.